Research Paper | Computer Science | E-ISSN No : 2454-9916 | Volume : 7 | Issue : 1 | Jan 2021

STUDY OF BIOMETRICS RECOGNITION SYSTEM WITH ITS ADVANTAGES AND DISADVANTAGES

*Manisha K. Borse[1] | Chetna A. Desale [1] | Deepak S. Dandwate[1] | Umesh J. Tupe[1]

[1]Department of Computer Science, Panchavati College of Management & Computer Science, Nasik, India.
(*Corresponding Author)

ABSTRACT

Now day's security of any area is most important task. At different places security required authentication for that purpose biometric system is commonly used. Biometrics is the most suitable means of identifying and authenticating individuals in a reliable and fast way through unique biological characteristics. In this paper we study some concepts which are related to biometrics like meaning of biometrics, history of biometrics, biometric verification and identification, Biometric Recognition techniques, uses, advantages, disadvantages of biometrics.

In the current research work we are focus different types of biometric system with its advantages and disadvantageous.

KEYPOINT: Biometrics, biometrics verification, Face, Fingerprint, Iris, voice recognition.

INTRODUCTION:
Today's life is full of trouble due to crime & corruption. So for safety we should have kind of Identification system. Biometrics is seen by many as a solution to a lot of the user identification and security problems in today's networks. Password abuse and misuse, intentional and inadvertent is a gaping hole in network security. This results mainly from human error and carelessness. Biometrics removes human error from the security equation. Biometric system is going to provide a better replacement for passwords and smartcards for securing applications. Biometrics is the most suitable means of identifying and authenticating individuals in a reliable and fast way through unique biological characteristics. Biometric systems can be operated in two modes, named identification and verification [9] "Biometrics is the identification or verification of human identity through the measurement of repeatable physiological and behavioral characteristics. Biometrics is body measurements and calculations related to human characteristics [1].

An early cataloguing of fingerprints dates back to 1881 when Juan Vucetich started a set of fingerprints of criminals in Argentina [2]. Nitzan Lebovic and Josh Ellenbogen argued, Alphonse Bertillon developed biometrics originated in the identification systems of criminal activity (1853–1914) and by Francis Galton's physiognomy and theory of fingerprints [3]. Lebovic, Galton's work on "led to the application of mathematical models to Psychology, fingerprints and facial characteristics", as part of "absolute identification" and "a key of inclusion and exclusion" of populations [4]. The biometric system is the absolute political weapon of our era" and a form of "soft control [5]. The theoretician David Lyon showed that during the past two decades biometric systems have penetrated the civilian market, and blurred the lines between governmental forms of control and private corporate control [6]. Kelly A. studied the objects or events that have no necessary connection come together and a new discourse formation is established: automated facial recognition as a homeland security technology [7].

Biometric Recognition:
Biometric recognition is an information system that allows the identification which is based on physiological and behavioral characteristics.

It consists of hardware systems for data acquisition, for storing purpose software components are used. For designing of recognition system different mathematical algorithms are implemented for different techniques, for data analysis data analyzers and reconstructions are used [8].

Biometric are based on following characteristics:

1. Physiological characteristics: fingerprints, height, weight, color and size of the iris, the retina, the shape of the ear, the physiognomy of the face, the shape of the hand.

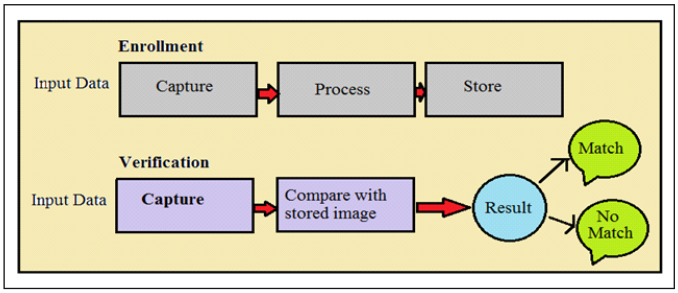
2. Behavioral characteristics: the vocal imprint, the movements of the body, the writing, the typing style on the keyboard, the style and the trend of the walk [8].

Identification or verification:
Depending on the objective functioning of the biometric recognition systems varies, which can be the identification or verification of a person:

- **Identification:** In identification system one too many matching techniques is used. The biometric recognition is done by matching the image, the data, the information acquired in real time with all the images and information present in a collection. The biometric recognition system will include identity by comparing and identifying the most similar and consistent physiological and behavioral characteristics between those in the collection and those collected in real time.

- **Verification:** one by one matching techniques is used in verification process, a person declares his identity. Verification process that requires a matching between the acquired data in real time from the sensors and that present in an archive [8].

Working of biometric system:
Biometric systems require two steps shown in Fig. 1:



1. Enrollment:
The system consists of the following steps:

a) Biometric scanners are used to acquire input signal.

b) By using digital signal processing, process on that input signal

c) Store that signal.

2. Verification:
The system consists of the following steps:

a) Biometric scanners are used to acquire input signal.

b) By using digital signal processing ,process on that input signal

c) Compared the current input signal with enrolled signal.

Biometric Recognition Techniques:
1. **Fingerprint Recognition:** Fingerprint recognition refers to the automated method of verification of a matching between two human fingerprints. The minutia and pattern classes of algorithms are used for recognition and opti-

cal, ultrasonic, passive capacitance and active capacitance type of sensors are used for Fingerprint recognition [11].

2. **Face Recognition:** In facial recognition system, the shape and position of different parts of the face are used to determine a match,

3. **Iris Recognition:** In iris recognition, a scanner reads the unique characteristics of an iris; scanner converted those characteristics into an encrypted code form [13].

4. **Voice Recognition:** In voice recognition, a sound is created by physical characteristics such as vocal tracts, mouth, nasal cavities and lip. The template is store in database and compare at the time of matching,

5. **Keystroke:** Keystroke is a behavioral biometric; in it observe the typing pattern [15].

Table 1: Different sensors used for different biometric systems.

Sr.	Biometrics systems	Sensors used for Acquisition
1	Fingerprint	Ink+ paper + scanner
		Optical sensor
		Capacitive sensor
		Ultrasound sensor
2	Face	Photo camera
		Video-camera
3	Speech	Microphone
4.	Iris	Desktop cameras
5	Keystroke	Keyboard

Table 1 show that different biometric system requires different sensing devices for sensing the data. For fingerprint detection system used the sensor Ink+ paper + scanner, optical sensor, capacitive sensor, ultrasonic sensor. Ink+ paper + scanner is the old technology. For Face recognition Photo camera or Video camera is used for sencing the data. For speech recognition microphone is use. For iris recognition desktop cameras are used. In keystroke system a keyboard is used as a sensing device. Now days in smart phone as well as authentication systems are designed by using different sensors. Different sensors have their different characteristics.

Table 2: Advantages and disadvantages of different biometric technology.

Sr. No.	Biometric technology	Advantages	Disadvantages
1	Face	setup on computers with a webcam Non-intrusive High social acceptance Cheap easy to setup	2D face recognition can be insecure and prone to spoofing Changes in hairstyle, makeup, facial hair, etc. Addition or removal of glasses, hats, scarf, etc. Due to sun exposure, skin color may change
2	Fingerprint	Low implementation cost Most developed biometric identification method High level of accuracy Easy to setup and use	For effect of dry, wet, dirty fingers, performance can change Some fingerprint scanners cannot acquire fingerprints that are too oily, dry, wet, warm, etc Temporal or permanent damages can make fingerprint recognition impossible.
3	Iris	High accuracy Hard to spoof Newer system can scan iris from a distance	Intrusive Expensive to setup Eye trauma is rarely present, but still possible. Although this system is quite robust, it is not popular nor the sensors are widely-introduced.
4	voice	Non-intrusive high social acceptability Cheap, does not require any expensive hardware or setup	The behavioral part changes over time due to age, medical conditions and emotional state. May not be suitable for high security applications when used as only method of identification Identity verification may take some time

CONCLUSION:

Biometric system is its own advantages and disadvantages over different recognition system. For designing of biometrics systems different sensors are used they are design by their application. For security, flexibility, scalability, easy to used, improving data accuracy biometrics are used everywhere.

ACKNOWLEDGEMENT

We are very much thankful to M.G. V's Panchavati College of Management & Computer Science, Nasik for providing lab facility with computer and internet, we especially thanks to Principal of our college, for his constant guidance and extensive support to encourage for this work.

REFERENCES:

I. https://en.wikipedia.org/wiki/Biometrics
II. The History of Fingerprints Archived 12 March 2013 at the Wayback Machine.
III. Josh Ellenbogen, Reasoned and Unreasoned Images: The Photography of Bertillon, Galton, and Marey (University Park, PA), 2012.
IV. Nitzan Lebovic, "Biometrics or the Power of the Radical Center", in Critical Inquiry 41:4 (Summer), 841–868, 2015.
V. Nitzan Lebovic, "Biometrics or the Power of the Radical Center", in Critical Inquiry 41:4 (Summer), p. 853, 2015.
VI. David Lyon, Surveillance Society: Monitoring Everyday Life (Philadelphia, 2001).
VII. Kelly A. Gates, Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance (New York), p. 100, 2011.
VIII. https://medium.com/iquii/biometric-recognition-definition-challenge-and-opportunities-of-biometric-recognition-systems
IX. https://www.researchgate.net/publication/3278329
X. Kresimir Delac , Mislav Grgic , "a survey of Biometric recognition methods
XI. https://www.biometricupdate.com/service-directory/fingerprint-recognition
XII. www.biometrics.org
XIII. https://www.recogtech.com/
XIV. Faundez-Zanuy, Marcos. "Biometric security technology." Encyclopedia of Artificial Intelligence. IGI Global. 262-269, , 2009
XV. Delac, Kresimir, and Mislav Grgic. "A survey of biometric recognition methods." Proceedings. Elmar-2004. 46th International Symposium on Electronics in Marine. IEEE, 2004.